

## REMARKS

The following remarks are responsive to the Final Office Action of December 30, 2009 (*Office Action*).

At the time of the *Office Action*, claims 1–23 were pending. The status of the claims is as follows:

- **Claims 1–23** stand rejected under **35 U.S.C. § 101** as being directed towards non-statutory subject matter; and
- **Claims 15 and 16** stand rejected under **35 U.S.C. § 112, second paragraph**, as being indefinite.

The Examiner also made a request for additional information under 37 C.F.R. § 1.105. Applicants thank the Examiner for his efforts and willingness to work with Applicants' representative during the telephone interview. Based on the constructive comments of the Examiner, Applicants have amended the application and respond to the *Office Action*, as follows.

Applicants have amended claims 1 and 15–17 herein in order to more distinctly claim the invention and address the issues raised by the Examiner.

### REQUEST FOR INFORMATION UNDER 37 C.F.R. § 1.105

In the Office Action, on p. 2, the Examiner requested additional information from the Applicants. Applicants formally and respectfully respond as follows:

#### **Inquiry A.1**

Applicants are not aware of any publication which taught the use of padding zeros between ones to avoid using a multiplication operation at the time of the invention.

#### **Inquiry A.2**

Applicants are not aware of any use of padding zeros between ones to avoid using a multiplication operation in applications other than cryptography at the time of the invention.

#### **Inquiry B**

No such publication exists.

**Inquiry C**

No such publication exists.

**Inquiry C**

No such publication exists.

**35 U.S.C. §101, NON-STATUTORY SUBJECT MATTER OF CLAIMS 1–23**

In the Office Action, on pp. 4–5, the Examiner rejected claims 1–23 as being directed towards non-statutory subject matter. Namely, the Examiner suggested that there was no particular machine recited, and that the claims were mere mathematical algorithms.

In response, Applicants have amended the independent claims to require the inclusion of both an integrated circuit card that therefore directs the subject matter to a machine, and further requires a utilization of the part of the cryptographic value in a practical application directed to a cryptographic exchange of information or a cryptographic security operation. Support for these amendments can be found at least in paragraphs 0001–0003, 0014–0025, and Figure 7 of the published application.

All other claims in the application depend from the independent claims, and are therefore contain statutory subject matter based on the arguments above and based on their dependency from one of the independent claims.

Based on these amendments and the understanding reached between the Examiner and Applicants' representative during the telephone interview, Applicants respectfully assert that the amendments overcome the rejection based on 35 U.S.C. § 101, and request that the Examiner withdraw this rejection from the application.

**35 U.S.C. §112, SECOND PARAGRAPH, INDEFINITENESS OF CLAIMS 15 AND 16**

In the Office Action, on pp. 5–6, the Examiner rejected claims 15 and 16 under 35 U.S.C. § 112, second paragraph, as being indefinite. Namely, the Examiner indicated that the cryptographic value (y) was not found to have been produced, but only a part of it, and therefore, it was unclear how the part of the cryptographic value relates to (y).

In re Appln. of Girault et al.  
Application No. 10/590,794  
RCE & Response to Final Office Action of December 30, 2009

In response, Applicants have amended claims 15 and 16 to indicate that the cryptographic value (y) is used for authenticating a device (claim 15) or used as an electronic signature (claim 16).

As discussed in paragraph 0046 of the published application, the cryptographic value (y) can be represented as a product of two factors with possibly a random number added to it. The calculation of a partial value of the cryptographic value (y) can therefore be utilized in determining the overall cryptographic value (y) that is ultimately used in a cryptographic or authenticating application. Applicants understood the Examiners comments during the telephone interview to indicate that these amendments would suffice to overcome the 35 U.S.C. § 112 rejections, and therefore, Applicants respectfully request that this rejection be withdrawn from the application.

### **Conclusion**

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call Applicants' undersigned representative(s).

Respectfully submitted,

/Mark Bergner/

Brian C. Rupp, Reg. No. 35,665  
Mark Bergner, Reg. No. 45,877  
DRINKER BIDDLE & REATH LLP  
191 North Wacker Drive, Suite 3700  
Chicago, Illinois 60606-1698  
(312) 569-1000 (telephone)  
(312) 569-3000 (facsimile)  
Customer No.: 08968

Date: May 27, 2010

CH01/ 25547767.1